

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-157554

(43)Date of publication of application : 31.05.2002

(51)Int.Cl. G06K 17/00
G06F 9/46
G06F 12/14
G06K 19/073

(21)Application number : 2001-220865 (71)Applicant : FUJITSU LTD

(22)Date of filing : 23.07.2001 (72)Inventor : KURITA YUKIYOSHI

(30)Priority

Priority number : 2000269096 Priority date : 05.09.2000 Priority country : JP

(54) SYSTEM FOR MANAGING ACCESS OF SMART CARDSHARING METHOD AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an access management system and a managing method for a smart card which give an authentication permission to each application (process) in regard to accesses by a plurality of applications.

SOLUTION: The applications 21 including a plurality of pieces of access processing to the smart card make an exclusion acquisition request to an exclusion control mechanism 11 at the time of making an access request to the smart card 22 in each access processing and requests access to an access control mechanism 12 when the applications 21 obtain exclusion. The mechanism 12 requests an input of a PIN(personal identification number) when the concerned application 21 is not authenticated and allows the application 21 to access the smart card 22 when the application 21 has already obtained authentication. The application 21 performs exclusion acquisition request/release in an access processing unit.

CLAIMS

[Claim(s)]

[Claim 1]An access control system of a smart card which manages access to a smart card by two or more applications characterized by comprising the following.

An exclusive control means which will be made finishing [exclusion acquisition of this application] if a logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to an exclusion acquisition request to a smart card from application.

As opposed to an access request to said smart card from application [finishing / application / exclusion acquisition]An access control means to which access to this smart card is permitted to application [finishing / application / this exclusion acquisition] when application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[Claim 2]If a logical channel [finishing / a logical channel / exclusion acquisition] does not exist in this smart card with other applications to an exclusion acquisition request to a smart card from applicationsaid exclusive control meansThe access control system according to claim 1 registering into cue application which performed this exclusion acquisition request.

[Claim 3]The access control system according to claim 1 or 2 characterized by refusing a demand of this application when said access control means has not attested application which gained said exclusion from said smart card to said access request.

[Claim 4]An access control system given in any 1 of claims 1 thru/or 3 when said access control means is extracted [said smart card] from a smart card readerwherein it changes application [finishing / application / attestation] into un-attesting with this ***** smart card.

[Claim 5]When said application carries out multiple-times access at said smart cardAn access control system given in any 1 of claims 1 thru/or 4 carrying out said exclusion acquisition request to said exclusive control means at the time of a start of each accessand carrying out a notice of release of exclusion to said exclusive control means at the time of an end of this access of each.

[Claim 6]To an exclusion acquisition request to a smart card from applicationwith other applicationsif this smart card is already ending with exclusion acquisitionsaid exclusive control meansThe access control system according to claim 5 using finishing [exclusion acquisition of application which registers into cue application which performed this exclusion acquisition requestand is registered into said cue to a notice of release of exclusion from said application].

[Claim 7]Said access control means receives a notice of attestation release of a smart card from applicationAn access control system given in any 1 of claims 1 thru/or 6wherein this attestation release requires attestation release of this smart card with this smart card at the time from the last application [finishing / the

application / attestation].

[Claim 8]It is a sharing method of a smart card which manages access to a smart card by two or more applicationsIf a logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to an exclusion acquisition request to a smart card from applicationAs opposed to an access request to said smart card from application [finishing / finishing / exclusion acquisition of this application / is used and / application / exclusion acquisition]A sharing method permitting access to this smart card to application [finishing / application / this exclusion acquisition] when application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[Claim 9]They are application including two or more access processings to one smart cardor its libraryAn exclusion acquisition request is performed to two or more access processingsrespectively at the time of a start of this access processingApplication characterized by performing an authentication demand to a smart card which exclusion gives a release notice and performs this access processing only at the time of processing of the beginning of said two or more access processingsrespectively at the time of an end of each access processingor its library.

[Claim 10]When used by an information processor in which two or more applications carry out parallel operationIf a logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to an exclusion acquisition request to a smart card from applicationAs opposed to an access request to said smart card from application [finishing / finishing / exclusion acquisition of this application / is used and / application / exclusion acquisition]When application [finishing / application / this exclusion acquisition] is already attested from this smart cardA recording medium which said information processor which memorized a program to which it makes it carry out to said information processor to permit access to this smart card to application [finishing / application / this exclusion acquisition] can read.

[Claim 11]When it performs with an information processor in which two or more applications carry out parallel operationIf a logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to an exclusion acquisition request to a smart card from applicationAs opposed to an access request to said smart card from application [finishing / finishing / exclusion acquisition of this application / is used and / application / exclusion acquisition]A program which it makes it perform to said information processor to permit access to this smart card to application [finishing / application / this exclusion acquisition] when application [finishing / application / this exclusion acquisition] is already attested from this smart card.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the access control of the smart card at the time of [which is depended on two or more processes of the data on a smart card] sharing.

[0002]

[Description of the Prior Art] The use to various fields from the data of very big capacity being memorizable as compared with the magnetic card used conventionally etc. is considered or the smart card is put in practical use.

[0003] The smart card equips the inside with CPU with the memory.

Since it accesses to the data in a memory via this CPU by making authenticating processing perform to CPU at the time of access, high security nature can be realized compared with the conventional magnetic card and this point also serves as a merit of the smart card.

[0004] The smart card has a security function by PIN (Personal Identification Number). It is possible to control to compare PIN with this function and to be able to access the confidential information in a card only when attested. The attestation by this PIN is what is called a password input method; the user using a smart card enters a password as PIN and it compares within the password and card which have memorized this in a smart card and when in agreement, access to an in-house data is permitted.

[0005] Access to a smart card is performed through the logical channel which a smart card has and an authentication demand is performed to a logical channel. And the smart card holds the states about security such as an authentication state by PIN for every logical channel of this.

[0006] Drawing 15 shows the logical construction inside the smart card seen from application. Within the smart card, data is managed by composition of a tree structure and DF (Delicated File) is provided in the unit for every application used for the lower layer of DIR in the top etc. And in each DFEF (Elementary File) holding actual data is stored. When accessing data from a smart card after application sends the positioning information which shows the position of the data accessed first and moves an access position to the target EF it performs read-out/writing of data from the EF. Each channel holds the present access position as state information.

[0007]

[Problem(s) to be Solved by the Invention] The usage which uses the present smart card simultaneously with two or more applications is examined. For example, the PKI (PublicKey Instructure) system which used the public-key crypto system as the base is built. When two or more applications are working by computer on this system it is considered as the one directions for the present smart card that each application

uses a smart card for the security authentication by a digital signature etc.

[0008]In this case two or more applications on the computer which connected the smart card will share a smart card. And since the number of the logical channels which one smart card has is about at most two when making much applications access to the same card the necessity that two or more applications share one logical channel comes out. For simplification of explanation the following explanation in a **** specification is premised on one application comprising one process is synonymous with a process and uses the word "application." Usually although one application comprises one process in many cases if application is replaced with a process and considered even when it comprises two or more processes the following explanation is fundamentally the same.

[0009]In the security system of the present smart card. If PIN attestation is performed to a logical channel with one application and an access permit is obtained from the logical channel not only the application that received attestation but other applications will be able to be henceforth accessed until attestation is canceled.

[0010]If it considers sharing the same information on one card between two or more applications from a viewpoint of security it will become firmer [it / to perform attestation by PIN for each application of every / a security level]. However in the access control to the present smart card. Since attestation is performed for every logical channel and an authentication state (was the access permit given or not?) is held at each logical channel when two or more applications share one logical channel if one application performs attestation by PIN and obtains an access permit access of other applications to a card from the logical channel will be attained without receiving attestation by PIN.

[0011]As mentioned above when each application accesses the data in a card after it transmits positioning information to a logical channel and moves an access position it performs writing/read-out of data but. When two or more applications share a logical channel as for each application grasp of the access position of KARENTO becomes difficult.

[0012]In view of the above-mentioned problem this invention to access by two or more applications (process) by managing the authentication state to a smart card in a unified manner Let it be a technical problem to provide the access control system and controlling method of a smart card which give attestation permission to each application (process) of every. each application (process) -- each time -- let it be a technical problem to provide the access control system and controlling method which are realized without enlarging the overhead according attestation to authenticating processing.

[0013]

[Means for Solving the Problem]In order to solve the above-mentioned problem an access control system of a smart card by this invention manages access to a smart card by two or more applications and is provided with an exclusive control means and

an access control means.

[0014]An exclusive control means will be taken as finishing [exclusion acquisition of this application]if a logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to an exclusion acquisition request to a smart card from application. The above-mentioned exclusive control means registers into cue application which performed this exclusion acquisition requestif a logical channel [finishing / a logical channel / exclusion acquisition] does not exist in this smart card with other applications to an exclusion acquisition request to a smart card from application.

[0015]As opposed to an access request to the above-mentioned smart card from application [finishing / an access control means / application / exclusion acquisition]When application [finishing / application / this exclusion acquisition] is already attested from this smart cardaccess to this smart card is permitted to application [finishing / application / this exclusion acquisition]. An access control means requires an input of PIN of this applicationwhen not having attested application which gained the above-mentioned exclusion from the above-mentioned smart card to the above-mentioned access request. Attestation of a smart card by each application was performed through this access control meansand an access control means grasps attestation relation between each application and a smart card.

[0016]Since exclusive control to a smart card is performed by exclusive control means according to this inventioneven if it shares a smart card with two or more applicationsattestation for every application is enabled.

[0017]It is judged by an access control means whether it is finishing [attestation of application which performed each access request]and since an access permit is given without performing authenticating processing when it is ending with attestationthe number of times of authenticating processing is reducible.

[0018]

[Embodiment of the Invention]One embodiment of this invention is described belowreferring to drawings. In order to give attestation permission for every applicationExclusive control is performed to a smart card (it is a logical channel when a smart card has two or more logical channels)While one attested application is using the smart cardthe application needs to monopolize a card (or logical channel)and needs to deter access from other applications. By following embodimentseach smart card is considered as composition provided with one logical channel for explanation simplification. When a smart card is provided with two or more logical channelsexclusive control explained below is performed per logical channel.

[0019]Drawing 1 establishes an exclusive control mechanism and shows the case where the exclusive operation of the application which accesses a smart card is performed. In drawing 1the exclusive control mechanism 11 is established between two or more applications 21 and the smart card 22When requiring access from the smart card 22each application 21 performs an exclusion acquisition request to this

exclusive control mechanism 11 and the application 21 with which exclusion was obtained accesses it by monopolizing the smart card 22. The exclusive control mechanism 11 of the figure has managed the exclusion to access to two cards of the cards a and b. And the three applications the application 1 the application 2 and the application 3 21 have published the access request to the card a and the exclusive control mechanism 11 is considered as exclusion acquisition to the application 1 of them and it changes other applications 2 and 3 into the waiting state until the card a is released. The application 1 which gained exclusion performs read-out/writing of data after performing PIN attestation to the logical channel of the card a. The application 21 besides during this period cannot be accessed to the card a. If processing of the application 1 is completed and the card a is released next the application 2 which is in the waiting state will gain exclusion and will access the data inside backward [which performed PIN attestation to the card a]. Thus by establishing the exclusive control mechanism 11 only one application which received attestation can be accessed to a smart card and attestation for every application 21 can be realized.

[0020] Since in the case of the method by the composition of this drawing 1 this smart card 22 is monopolized by this application 21 while the one application 21 is using the smart card 22 other applications 21 will be in a waiting state until exclusion is canceled and the smart card 22 is released. Therefore in this method the parallel processing performance of two or more applications is bad and user-friendliness worsens dramatically -- the application in a waiting state is visible to the state where suspended long period processing and it hung-up.

[0021] There is a method which releases in detail the smart card 22 which the application 21 monopolized as what avoids this when the access processing to the smart card 22 was completed. In this method when the application 21 includes the access processing to the multiple-times smart card 22 exclusion acquisition / release to the smart card 22 are performed to the exclusive control mechanism 11 for every access processing and exclusive control is divided briskly.

[0022] The example of the exclusion acquisition / release to the smart card of each application by this method is shown in drawing 2. The figure is what shows the example of access processing to the smart card of each application when the three applications the application 1 the application 2 and the application 3 21 publish an access request to the card a like drawing 1. As for arrow ** from the exclusion acquisition request from each application 21 to the exclusive control mechanism 11 and the exclusive control mechanism 11 arrow ** to the exclusive control mechanism 11 in the said figure shows the notice of the exclusion acquisition to each application 21 from the exclusive control mechanism 11. The PIN authenticating processing according [a shadow area] to each application 21 and a shading portion show access processing to the smart card 22.

[0023] When the application 21 which gained exclusion canceled exclusion and does

not release the smart card 22 until all the processings were completed. To the position of 33 which processing of the application 1 which has already gained the exclusion to the card a completes from the position of 31 in drawing 2 which carried out the exclusion acquisition request to the card a to the exclusive control mechanism 11 the application 2 will be in a waiting state until processing of this application 2 completes the application 3 from the position of 32. However since another application 21 in the period of which exclusion was canceled when the application 21 divided exclusive control briskly for every access processing as shown in the figure can access the card a. The period which will be in the waiting state for exclusion acquisition and processing stops becomes short and the parallelism of processing improves.

[0024] Thus if exclusive control is changed frequently the period of the waiting state of each application will become short and the parallelism of processing will improve. However as shown in the slash part of drawing 2 each application will need to perform setting-out/release processing of an authentication state to the degree of a change and the overhead for it will become large. Since PIN is transmitted when obtaining re-permission of attestation each application 21 will continue holding PIN and also produces the problem of security. In order to avoid this if a user uses the degree of authenticating processing with the composition which enters a password the overhead of authenticating processing will become large further.

[0025] The composition in consideration of this point is shown in drawing 3. In the composition of drawing 3 between two or more applications 21 and the smart card 22 the exclusive control mechanism 11 is performing the exclusive operation of the application 21 which accesses the smart card 22 forming the access controller 12 in addition to the exclusive control mechanism 11 and managing attestation by the smart card 22 of each application 21 in a unified manner by this access controller 12.

[0026] When each application 21 requires access from the smart card 22 if it performs an exclusion acquisition request to the exclusive control mechanism 11 first and exclusion can be gained it will request the attestation to the smart card 22 from the access controller 12 next. And if attestation is obtained the data in the smart card 22 will be accessed.

[0027] The access controller 12 has an authentication state management table. The authentication state of each application and the smart card 22 is managed about between after the application 21 makes a start declaration of the attestation to the smart card 22 using this authentication state management table until it notifies release of attestation.

[0028] Drawing 4 is a figure showing the example of composition of an authentication state management table. An authentication state management table is a table which uses from which smart card 22 each application 21 has obtained attestation now in order that the exclusive control mechanism 11 may manage and has matched and memorized application identification information and attested card information. What cannot operate the application with this general identifier in which application

identification information memorizes an identifier [meaning / for identifying each application 21] is used for example it is added to each process at a process generate time and the process ID which the kernel has managed is used. Or it is good also as composition in which the access controller 12 carries out generation addition for an identifier one by one to the application 21 which performed the access request to access to a smart card.

[0029] Drawing 4 has illustrated the case where the authentication state of each application 21 to the two smart cards 22 of the cards a and b is managed and the card with which the application 21 is attested as attested card information to each application is recorded. The portion of a blank shows that the smart card [finishing / to the application / attested card information / a smart card / attestation] does not exist. Finishing [the application 1 / the card a and b both / ending with attestation the application 2 and the application n / un-attesting and the application 3 / the card a / attestation] in the figure all.

[0030] Each application 21 performs access to the attestation and the smart card 22 to the smart card 22 via the access controller 12. If there is an access request from the application 21 to the smart card 22 it is investigated whether it is ending with attestation to the smart card 22 in which the application 21 carried out the access request with reference to the authentication state management table. If it has not attested the demand from the application 21 will be refused and the input of PIN is required of the application 21 and authenticating processing with the smart card 22 is performed. If the application 21 is ending with attestation since the application 21 has already obtained attestation permission of the smart card 21 it will permit and perform access to the smart card 21.

[0031] Drawing 5 is a figure showing the flow of processing of the application 21 at the time of the application 21 performing access to the smart card 22 the exclusive control mechanism 11 and the access controller 12. The figure makes the example the case where the application 1 accesses to the card a and 1-23 under following explanation correspond with the number in drawing 5.

- 1) The application 1 performs an exclusion acquisition request to the exclusive control mechanism 11 in order to perform the exclusion start to the card a.
- 2) To the demand from the application 1 the exclusive control mechanism 11 investigates whether there is any application exclusion gained to the card a and if other applications have already gained it will register it into the cue of the waiting for exclusion. If it is not exclusion acquisition settled exclusion acquisition will be notified to the application 1.
- 3) The application 1 makes an access start declaration to the card a to the access controller 12.
- 4) The access controller 12 registers the application 1 into an authentication state management table to access start declaration. And the input request of PIN is performed to the application 1. When the application 1 is making an access start

declaration to the card b since the application 1 is already registered into the authentication state management table it is not necessary to register it into an authentication state management table again by the access start declaration to the card a.

5) The application 1 demands the input of a password from a user specifies PIN from a user's input and requires the attestation to the card a.

6) The exclusive control mechanism 11 notifies PIN to the card a and makes an authentication check perform on the card a.

7) The access controller 12 will register that the application 1 is ending with attestation at the card a into an authentication state management table if attestation is obtained as a result of the authentication check by the card a.

8) The application 1 requires read-out/writing of the data to the card a from the access controller 12.

9) An authentication state management table is searched to read-out/write request from the application 1 and if the application 1 is ending with attestation it will access the attested card a to the card a. If it has not attested an error will be notified to the application 1.

10) When one access processing is completed and it cancels monopoly of the card a the application 1 notifies release of exclusion to the exclusive control mechanism 11.

11) The exclusive control mechanism 11 deletes the exclusion acquisition to the card a of the application 1 registered and if there is the application 21 otherwise registered into the cue of the waiting for the exclusion to the card a it will register exclusion acquisition of the application 21.

12) The application 1 performs processing of those other than the access processing to the card a after release of exclusion. Since the exclusion of the card a is released in the meantime other applications 21 can use the card a.

13) The application 1 will carry out an exclusion acquisition request to the exclusive control mechanism 11 if the necessity for access to the card a arises again.

14) finishing [it investigates again whether the exclusive control mechanism 11 has like 2 the application exclusion gained to the card a to the demand from the application 1 and / other applications / exclusion acquisition] already -- it is not -- if -- notify exclusion acquisition to the application 1.

15) The application 1 requires read-out/writing of the data to the card a from the access controller 12.

16) The access controller 12 performs the again same processing as 9. Since it is registered into the authentication state management table by 7 at this time that the application 1 is ending with attestation at the card a a card a hair KUSESU is performed as it is. Processing for the number of times 10-16 of the access processing to the card a in the application 1 is repeated henceforth.

17) If all the access processings are completed the application 1 will notify release for the attestation to the card a to the access controller 12.

- 18) The access controller 12 deletes the information card a attested from the application 1 of an authentication state management table.
- 19) The access controller 12 will require attestation release of the card a if an authentication state is held and the application 21 attested stops existing until the application 21 otherwise attested by the card a stops existing in the authentication state management table 13. Thereby the number of times of authenticating processing with the same smart card is reducible.
- 20) The application 1 notifies the end of access to the smart card 22 to the access controller 12.
- 21) If the notice by 20 is received the access controller 12 will delete the application 1 from an authentication state management table. When the application 1 has not ended access yet to other smart cards 22 at this time the application 1 is not deleted from an authentication state management table.
- 22) The application 1 notifies release of the exclusion of the card a to the exclusive control mechanism 11.
- 23) The exclusive control mechanism 11 performs the again same processing as 11 and cancels exclusion.

[0032] Drawing 6 is a figure showing the processing to the smart card of each application by the composition provided with the exclusive control mechanism 11 and the access controller 12 of drawing 3. The figure has shown processing of the same application 21 under the same premise as drawing 2 for comparison. As compared with drawing 2 drawing 6 each application 21 It is only performing authenticating processing by PIN at the time of the access processing start to the very first card a and release processing of the attestation at the time of the very last end of access processing to the card a as authenticating processing and the authenticating processing for every access processing to the card a which was being performed is omitted in drawing 2. Therefore as for each application 21 the part processing time to which authenticating processing was abbreviated becomes short. The period when the period when each application 21 monopolizes the card a will also be in the state waiting for a part since only the part from which authenticating processing was excluded becomes short is short and may end. Since each application 21 should perform PIN attestation to the smart card 22 only once first if attestation is obtained from a card it can cancel PIN.

[0033] Drawing 7 is a flow chart which shows processing of the application 21 which accesses the smart card 22 by this system. Although the mechanism in which these processings are performed can also be made into the application 21 with the composition given directly general composition takes the gestalt which realizes these processings as a library and includes this library in each application 21.

[0034] When the application 21 accesses the smart card 22 it requests exclusion acquisition to the exclusive control mechanism 11 first (Step S1) and waits for the response from the exclusive control mechanism 11. As a result processing will be

ended if there is a notice of a purport which cannot gain exclusion from the exclusive control mechanism 11 for a certain reason (Step S2NO).

[0035]If there is a notice of an exclusion acquisition success from the exclusive control mechanism 11 to a request of exclusion acquisition (Step S2YES)a start declaration of access to the smart card 22 will be made to the access controller 12 as Step S3 next.

[0036]Access to this smart card 22 is access to the unattested smart card 22Since the attestation to the smart card 22 is requiredwhen the input of PIN is required from the access controller 12 (step S4YES)it checks by sending the password which the user entered as PIN as Step S8 to the access controller 12and requesting authenticating processing. Processing is endedif are attested as a result (step S9YES)and processing will be moved to Step S5it will access to a smart card and it will not be attested (step S9NO).

[0037]In step S4since the further authenticating processing does not have necessity when this access is access to the smart card 22 which has already obtained attestation (step S4NO)access to the smart card 22 is permitted as Step S5and read-out/writing of data are performed.

[0038]An end of the access processing of Step S5 will make an end declaration of access to the smart card 22 to the access controller 12 as Step S6. And as Step S7release of the exclusion to the smart card 22 is notified to the exclusive control mechanism 11and the access processing to the smart card 22 is ended.

[0039]Drawing 8 is a flow chart which shows the processing of the exclusive control mechanism 11 to the exclusion acquisition request from the application 21. If the exclusion acquisition request from the application 21 to the smart card 22 occursthe exclusive control mechanism 11 will judge whether it is ending with exclusion acquisition as Step S11 with the application 21 of others [smart card / 22 / of which exclusion acquisition was required] already. If exclusion acquisition by the application 21 besides the result is not performed (Step S11NO)it registers as finishing [exclusion acquisition of the smart card 22]exclusion acquisition is notified to the application 22 which requiredand processing is ended.

[0040]If other applications 21 are ending with exclusion acquisition at Step S11 (Step S11YES)this exclusion acquisition request will be added to the waiting cue for exclusion as Step S12and processing will be ended.

[0041]Drawing 9 is a flow chart which shows the processing of the exclusive control mechanism 11 to the notice of release of the exclusion from the application 21. If the notice of release of the exclusion from the application 21 to the smart card 22 is receivedthe exclusive control mechanism 11 will delete the registration as Step S21 in which the application 21 has been exclusion gainedand will cancel exclusion.

[0042]And if the application 21 which serves as waiting for exclusion to the smart card 22 which investigated the waiting cue for exclusionand of which exclusion was canceled exists (Step S22YES)After registering the exclusion acquisition to the smart

card 22 of the application 21 registered into the head of the waiting cue for exclusion and dispatching the smart card 22 and if waiting does not exist in the waiting cue for exclusion (Step S22NO) processing is ended as it is.

[0043] Drawing 10 is a flow chart which shows processing of the access controller 12 to the access request to the smart card 22 from the application 21. To the access start declaration from the application 21 as Step S31 the access controller 12 registers the application 21 into an authentication state management table and registers an access request process to the smart card 22.

[0044] Drawing 11 is a flow chart which shows processing of the access controller 12 to the access request to the smart card 22 from the application 21. The access controller 12 investigates whether the application 21 is already attestation settled from the smart card 22 of the access request point with reference to an authentication state management table as Step S41 to the access request from the application 21. As a result since the further attestation does not have necessity if it is already ending with attestation (Step S41YES) an access permit is notified to the application 21 as Step S45.

[0045] Since it is necessary at Step S41 to perform authenticating processing if the application 21 has not obtained attestation yet (Step S41NO) The input of a password is required of the application 21 as Step S42 and the authentication check by PIN is requested to the smart card 22. As a result if attestation is obtained from the smart card 22 an access permit will be notified to the application 21 as Step S45 and attestation will not be obtained (Step S43NO) access disapproval is notified to the application 21 and processing is ended.

[0046] Drawing 12 is a figure showing the composition of the system which uses the smart card in this embodiment. The access control system 40 which manages between the application 41 in this embodiment and the smart cards 42 is constituted between the smart card reader 43 and the library 44 of each application 41 and is realized in the form mounted in OS as one function of OS.

[0047] The application 41 performed altogether the authenticating processing and access processing to the smart card 42 via this access control system 40 and the access control system 40 grasps the exchange between each application 41 and the smart card 42. If the state of the smart card reader 43 is also grasped for example the smart card 42 is extracted from the smart card reader 43 the access control system 40 investigates an authentication state management table and if there is application which the card makes finishing [attestation] it will change it into un-attesting.

[0048] Although the access control system 40 has composition which has independently the exclusive control mechanism 11 and the access controller 12 in an inside it can also realize these as one functional constitution element. On security since two or more applications share an access controller and an exclusive control mechanism if it realizes in the kernel of OS they can improve security more.

[0049] Drawing 13 is a system environment figure of an information processor when a

computer program realizes the access control of the above-mentioned smart card in this embodiment. The information processor which mounted the smart card like drawing 13 CPU51ROMThe input/output devices (I/O) 54such as the main memory unit 52the auxiliary storage unit 53a displayand a keyboardLAN and WAN by RAMThe network connection apparatus 55such as a modem which performs other information processors and network connection by a general line etc.a diskIt had the smart card reader 58 which the medium readers 56 and 1 which read a memory content from the portable recording media 57such as magnetic tapethru/or plurality areand mounts the smart card 59and these are provided with the composition mutually connected by bus 60.

[0050]In the information processing system of drawing 13the program and data which are memorized by the recording media 57such as magnetic tapea floppy (registered trademark) diskCD-ROMand MOwith the medium reader 56 are readand this is downloaded to the main memory unit 52 or the hard disk 55. And each processing by this embodiment can be realized by softwarewhen CPU51 performs this program and data.

[0051]In this information processorexchange of application software may be performed using the recording media 57such as a floppy disk. Thereforethis invention can also be constituted as the recording medium 57 in which computer read-out for operating an above-mentioned embodiment of the invention as a computer is possiblewhen used not only by the access control system and sharing method of a smart card but by computer.

[0052]As shownfor example in drawing 14to a "recording medium" In this caseCD-ROMThe portable recording medium 76 which can be desorbed to the medium drives 77such as a floppy disk (or they may be MODVDa removable hard disketc.)The memory (RAM or hard disk) 75 grade in the memory measures (database etc.) 72 in the devices (server etc.) of the exterior transmitted by network line 73 course or the main part 74 of the information processor 71 is contained. The program memorized by the portable recording medium 76 and the memory measures (database etc.) 72 is loaded to the memories (RAM or a hard disk) 75 in the main part 74and is executed.

[0053](Additional remark 1) It is an access control system of the smart card which manages access to the smart card by two or more applicationsIf the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition request to the smart card from applicationAs opposed to the access request to said smart card from the exclusive control means made finishing [exclusion acquisition of this application] and the application [finishing / application / exclusion acquisition]The access control system equipping the application [finishing / application / this exclusion acquisition] with the access control means to which access to this smart card is permitted when the application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[0054](Additional remark 2) If the logical channel [finishing / a logical channel / exclusion acquisition] does not exist in this smart card with other applications to the exclusion acquisition request to the smart card from applicationsaid exclusive control meansAn access control system given in the additional remark 1 registering into cue the application which performed this exclusion acquisition request.

[0055](Additional remark 3) Access control system the additional remark 1 characterized by refusing the demand of this application when said access control means has not attested the application which gained said exclusion from said smart card to said access requestor given in 2.

[0056](Additional remark 4) Access control system given in any 1 of the additional remarks 1 thru/or 3wherein said access control means manages the attestation relation between application and a smart card using the process ID of this application.

[0057](Additional remark 5) Access control system given in any 1 of the additional remarks 1 thru/or 4 when said access control means is extracted [said smart card] from a smart card readerwherein it changes the application [finishing / application / attestation] into un-attesting with this ***** smart card.

[0058](Additional remark 6) When said application carries out multiple-times access at said smart cardAn access control system given in any 1 of the additional remarks 1 thru/or 5 carrying out said exclusion acquisition request to said exclusive control means at the time of the start of each accessand carrying out the notice of release of exclusion to said exclusive control means at the time of the end of this access of each.

[0059](Additional remark 7) To the exclusion acquisition request to the smart card from applicationwith other applicationsif this smart card is already ending with exclusion acquisitionsaid exclusive control meansAn access control system given in the additional remark 6 using finishing [exclusion acquisition of the application which registers into cue the application which performed this exclusion acquisition requestand is registered into said cue to the notice of release of the exclusion from said application].

[0060](Additional remark 8) Said access control means receives the notice of attestation release of a smart card from applicationAn access control system given in any 1 of the additional remarks 1 thru/or 7wherein this attestation release requires attestation release of this smart card with this smart card at the time from the last application [finishing / the application / attestation].

[0061](Additional remark 9) It is a sharing method of the smart card which manages access to the smart card by two or more applicationsIf the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition request to the smart card from applicationAs opposed to the access request to said smart card from the application [finishing / finishing / exclusion acquisition of this application / is used and / application / exclusion acquisition]A sharing method permitting access to this smart card to the

application [finishing / application / this exclusion acquisition] when the application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[0062](Additional remark 10) They are application including two or more access processings to one smart card or its library. An exclusion acquisition request is performed to two or more access processings respectively at the time of the start of this access processing. The application characterized by performing an authentication demand to the smart card which exclusion gives a release notice and performs this access processing only at the time of processing of the beginning of said two or more access processings respectively at the time of the end of each access processing or its library.

[0063](Additional remark 11) It is a library of application including two or more access processings to one smart card. An exclusion acquisition request is performed to two or more access processings respectively at the time of the start of this access processing. The library of the application performing an authentication demand to the smart card which exclusion gives a release notice respectively at the time of the end of each access processing and performs this access processing only at the time of processing of the beginning of said two or more access processings.

[0064](Additional remark 12) When used by the information processor in which two or more applications carry out parallel operation. If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition request to the smart card from application A as opposed to the access request to said smart card from the application [finishing / finishing / exclusion acquisition of this application / is used and / application / exclusion acquisition]. When the application [finishing / application / this exclusion acquisition] is already attested from this smart card. The recording medium which said information processor which memorized the program to which it makes it carry out to said information processor to permit access to this smart card to the application [finishing / application / this exclusion acquisition] can read.

[0065]

[Effect of the Invention] Since exclusive control to a smart card is performed according to this invention even if it shares a smart card with two or more applications, attestation of each application units is enabled.

[0066] Since the attestation relation between each application and a smart card is managed in a unified manner. Since authenticating processing will be performed only when it is judged whether it is finishing [the smart card / attestation of the application] and it has not attested if application performs an access request to a smart card. The number of times of authenticating processing can be reduced and the overhead by authenticating processing can be made small. Since authenticating processing by PIN is performed only once first, the application does not need to continue holding PIN and can aim at improvement in a security level.

[0067]Access of a smart card is attained among two or more attested applicationswith an authentication state held. The application can shorten the waiting state period for exclusion acquisition. Thereforethe parallelism of processing can be improved and shortening of the processing time of each application can be aimed at again.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the composition at the time of establishing an exclusive control mechanism and performing the exclusive operation of access to a smart card.

[Drawing 2]It is a figure showing the access processing to the smart card of each application at the time of the composition provided with the exclusive control mechanism.

[Drawing 3]It is a lineblock diagram at the time of providing an exclusive control mechanism and an access controller.

[Drawing 4]It is a figure showing the example of composition of an authentication state management table.

[Drawing 5]It is a figure showing the flow of processing of the application at the time of application performing access to a smart cardan exclusive control mechanismand an access controller.

[Drawing 6]It is a figure showing the access processing to the smart card of each application at the time of the composition provided with the exclusive control mechanism and the access controller.

[Drawing 7]It is a flow chart which shows processing of the application which accesses a smart card.

[Drawing 8]It is a flow chart which shows the processing of an exclusive control mechanism to the exclusion acquisition request from application.

[Drawing 9]It is a flow chart which shows the processing of an exclusive control mechanism to the notice of release of the exclusion from application.

[Drawing 10]It is a flow chart which shows processing of the access controller to the access start declaration to the smart card from application.

[Drawing 11]It is a flow chart which shows processing of the access controller to the access request to the smart card from application.

[Drawing 12]It is a figure showing the composition of the system which uses the smart card in this embodiment.

[Drawing 13]It is a system environment figure of an information processor.

[Drawing 14]It is a figure showing the example of a storage.

[Drawing 15]It is a figure showing the logical construction inside a smart card.

[Description of Notations]

- 11 Exclusive control mechanism
 - 12 Access controller
 - 21 and 41 Application
 - 2242and 59 Smart card
 - 40 Access control system
 - 43 and 58 Smart card reader
 - 51 CPU
 - 52 Main memory unit
 - 55 Auxiliary storage unit
 - 54 Input/output device
 - 55 Network connection apparatus
 - 56 Medium reader
 - 57 Portable storage
 - 60 Bus
 - 71 Information processor
 - 72 Memory measure
 - 73 Network line
 - 74 Information processor body (computer)
 - 75 Memory
 - 76 Portable recording medium
-

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-157554
(P2002-157554A)

(43) 公開日 平成14年5月31日 (2002.5.31)

(51) Int.Cl. ⁷	識別記号	F I	ターマコード* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	E 5 B 0 1 7
G 0 6 F 9/46	3 4 0	G 0 6 F 9/46	3 4 0 F 5 B 0 3 5
	12/14		3 1 0 K 5 B 0 5 8
G 0 6 K 19/073	3 1 0	G 0 6 K 19/00	P 5 B 0 9 8

審査請求 未請求 請求項の数11 O L (全 14 頁)

(21) 出願番号 特願2001-220865(P2001-220865)
(22) 出願日 平成13年7月23日 (2001.7.23)
(31) 優先権主張番号 特願2000-269096(P2000-269096)
(32) 優先日 平成12年9月5日 (2000.9.5)
(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号
(72) 発明者 栗田 享佳
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(74) 代理人 100074099
弁理士 大菅 義之 (外1名)
Fターム(参考) 5B017 AA07 BA06 CA14
5B035 AA13 CA11 CA29 CA38
5B058 CA23 CA26 KA02 KA04 YA20
5B098 AA03 GA01 GD03 GD15

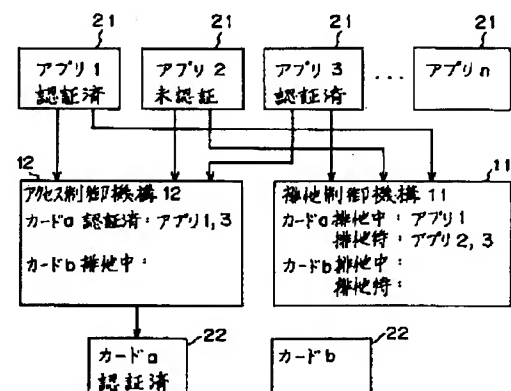
(54) 【発明の名称】 スマートカードのアクセス管理システム、共有方法及び記憶媒体

(57) 【要約】

【課題】 複数のアプリケーションによるアクセスに対し、各アプリケーション（プロセス）毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。

【解決手段】 スマートカードへの複数のアクセス処理を含むアプリケーション21は、各アクセス処理毎にスマートカード22に対してアクセス要求を行う際、排他制御機構11に対して排他獲得要求を行い、排他が得られるとアクセス制御機構12に対してアクセスを要求する。アクセス制御機構12はアプリケーション21が未認証ならばP I Nの入力を要求し、既に認証を得られていればスマートカード22へのアクセスを許可する。アプリケーション21はアクセス処理単位で排他獲得要求／解除を行う。

排他制御機構及びアクセス制御機構を
設けた場合の構成図



【特許請求の範囲】

【請求項1】 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段とを備えることを特徴とするアクセス管理システム。

【請求項2】 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする請求項1に記載のアクセス管理システム。

【請求項3】 前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒否することを特徴とする請求項1又は2に記載のアクセス管理システム。

【請求項4】 前記アクセス制御手段は、前記スマートカードがスマートカードリーダーより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする請求項1乃至3のいずれか1に記載のアクセス管理システム。

【請求項5】 前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする請求項1乃至4のいずれか1に記載のアクセス管理システム。

【請求項6】 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする請求項5に記載のアクセス管理システム。

【請求項7】 前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている

最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする請求項1乃至6のいずれか1に記載のアクセス管理システム。

【請求項8】 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【請求項9】 1つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであって、複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそのライブラリ。

【請求項10】 複数のアプリケーションが並列動作する情報処理装置によって使用された時、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【請求項11】 複数のアプリケーションが並列動作する情報処理装置によって実行された時、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許

可することを前記情報処理装置に行わせるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、スマートカード上のデータの複数プロセスによる共有した場合のスマートカードのアクセス管理に関する。

【0002】

【従来の技術】スマートカードは、従来用いられている磁気カードに比して非常に大きな容量のデータを記憶することが出来ることなどから、様々な分野への使用が検討され、あるいは実用化されている。

【0003】またスマートカードは、内部にメモリと共にCPUを備えており、このCPUを介してメモリ内のデータへアクセスを行うので、アクセス時にCPUに認証処理を行わせることにより、従来の磁気カードに比べて高いセキュリティ性を実現出来、この点もスマートカードのメリットとなっている。

【0004】スマートカードはPIN (Personal Identification Number) によるセキュリティ機能を持っており、この機能によりPINの照合を行い、認証された場合にだけカード内の秘密情報をアクセスすることができるよう制御することが可能である。このPINによる認証は、いわゆるパスワード入力方式で、スマートカードを用いるユーザがPINとして例えばパスワードを入力し、これをスマートカード内に記憶しているパスワードとカード内で比較して、一致した場合に内部データへのアクセスを許可する。

【0005】スマートカードへのアクセスは、スマートカードが持つ論理チャンネルを通して行い、認証要求は論理チャンネルに対して行われる。そしてスマートカードは、この論理チャンネル毎にPINによる認証状態などセキュリティに関する状態を保持している。

【0006】図15は、アプリケーションから見たスマートカード内部の論理的構成を示したものである。スマートカード内では、データをツリー構造の構成によって管理しており、最上位にあるDIRの下層に、使用されるアプリケーション毎の単位等でDF (Delicated File) が設けられている。そして、各DF内には実際のデータを保持しているEF (Elementary File) が格納されている。スマートカードからデータにアクセスする際、アプリケーションは、まずアクセスを行うデータの位置を示す位置付け情報を送って、目的のEFにアクセス位置を移動した後、そのEFからデータの読みだし／書き込みを行う。また各チャンネルは、現在のアクセス位置を状態情報として保持している。

【0007】

【発明が解決しようとする課題】現在スマートカードを複数のアプリケーションで同時に使用する使い方が検討されている。例えば公開鍵暗号方式をベースとしたPKI (Public Key Instructure) システムを構築し、この

システム上のコンピュータで複数のアプリケーションが稼動している場合に、各アプリケーションがデジタル署名などによるセキュリティ認証にスマートカードを用いることが、現在スマートカードの1つの使用方法として考えられている。

【0008】この場合、スマートカードを接続したコンピュータ上の複数のアプリケーションがスマートカードを共用することになる。そして1つのスマートカードが持つ論理チャンネルの数はせいぜい2チャンネル程度なので、多数のアプリケーションに同一のカードに対してアクセスさせる場合、1つの論理チャンネルを複数のアプリケーションが共有する必要があるが出てくる。尚本明細書内の以下の説明は、説明の簡略化のため、1つのアプリケーションは1つのプロセスで構成されることを前提としており、アプリケーションという言葉のプロセスと同義で用いている。通常1つのアプリケーションは1つのプロセスで構成されることが多いが、複数のプロセスで構成されている場合でも、アプリケーションをプロセスと置換えて考えれば、以下の説明は基本的に同じである。

【0009】現行のスマートカードのセキュリティ方式では、1つのアプリケーションがある論理チャンネルに対してPIN認証を行いアクセス許可を得ると、以降その論理チャンネルからは、認証が解除されるまでの間、認証を受けたアプリケーションだけでなく他のアプリケーションもアクセス出来てしまう。

【0010】複数のアプリケーションで1つのカードの同じ情報を共有することを、セキュリティの観点から考えると、個々のアプリケーション毎にPINによる認証を行った方がセキュリティレベルはより強固になる。しかし、現行のスマートカードへのアクセス制御では、1つの論理チャンネルを複数のアプリケーションで共有する場合、論理チャンネル毎に認証が行われ各論理チャンネルに認証状態 (アクセス許可を与えたか否か) が保持されるため、1つのアプリケーションがPINによる認証を行ってアクセス許可を得れば、他のアプリケーションはPINによる認証を受けずに、その論理チャンネルからカードへのアクセスが可能となってしまう。

【0011】また、上述したように各アプリケーションは、カード内のデータにアクセスする際、位置付け情報を論理チャンネルに送信してアクセス位置を移動してからデータの書き込み／読みだしを行うが、複数のアプリケーションが論理チャンネルを共有する場合、各アプリケーションはカレントのアクセス位置の把握が難しくなる。

【0012】上記問題点を鑑み、本発明は、複数のアプリケーション (プロセス) によるアクセスに対し、スマートカードへの認証状態を一元管理することにより、各アプリケーション (プロセス) 毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。また、各アプリケーション (プロセス) 毎の認証を認証処理によるオーバーヘッドを

大きくすること無く実現するアクセス管理システム及び管理方法を提供することを課題とする。

【0013】

【課題を解決するための手段】上記問題点を解決するため、本発明によるスマートカードのアクセス管理システムは、複数のアプリケーションによるスマートカードへのアクセスを管理するものであって、排他制御手段及びアクセス制御手段を備える。

【0014】排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在すれば、該アプリケーションを排他獲得済みとする。また上記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録する。

【0015】アクセス制御手段は、排他獲得済みとなっているアプリケーションからの上記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可する。またアクセス制御手段は、上記アクセス要求に対し、上記排他を獲得したアプリケーションが上記スマートカードから未認証である時、該アプリケーションにPINの入力を要求する。各アプリケーションによるスマートカードの認証はこのアクセス制御手段を通して行われ、アクセス制御手段は各アプリケーションとスマートカードとの認証関係を把握している。

【0016】本発明によれば、排他制御手段により、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション毎の認証を可能とする。

【0017】また、アクセス制御手段により、各アクセス要求を行ったアプリケーションが認証済みかどうか判断され、認証済みの場合、認証処理を行わずにアクセス許可を与えるので、認証処理回数を削減することが出来る。

【0018】

【発明の実施の形態】以下に本発明の一実施形態について、図面を参照しながら説明する。各アプリケーション毎に認証許可を与えるようにするためには、スマートカード（スマートカードが複数の論理チャンネルをもつ場合論理チャンネル）に対して排他制御を行い、認証された1つのアプリケーションがスマートカードを使用している間、そのアプリケーションがカード（若しくは論理チャンネル）を専有し、他のアプリケーションからのアクセスを抑止する必要がある。尚説明簡略化の為、以下の実施

形態では各スマートカードは論理チャンネルを1つ備える構成とする。尚スマートカードが複数論理チャンネルを備えた場合は、以下に説明する排他制御は論理チャンネル単位で行われる。

【0019】図1は、排他制御機構を設け、スマートカードにアクセスするアプリケーションの排他処理を行った場合を示す。図1では、複数のアプリケーション21とスマートカード22の間に排他制御機構11を設け、スマートカード22に対してアクセスを要求する際、各アプリケーション21はこの排他制御機構11に対して排他獲得要求を行い、排他が得られたアプリケーション21が、スマートカード22を専有してアクセスを行う。同図の排他制御機構11はカードa、bの2つのカードへのアクセスに対する排他を管理している。そしてアプリ1、アプリ2及びアプリ3の3つのアプリケーション21がカードaに対してアクセス要求を発行しており、排他制御機構11はそのうちのアプリ1に対して排他獲得とし、他のアプリ2及び3はカードaが解放されるまで待ち状態にしておく。排他を獲得したアプリ1は、カードaの論理チャンネルに対してPIN認証を行った後データの読みだし／書込みを行う。この間他のアプリケーション21は、カードaに対してアクセスすることが出来ない。アプリ1の処理を完了してカードaを解放すると、次に、待ち状態となっているアプリ2が排他を獲得し、カードaに対してPIN認証を行った後内部のデータにアクセスする。この様に排他制御機構11を設けることにより、認証を受けた1つのアプリケーションのみスマートカードに対してアクセスすることが出来る。各アプリケーション21毎の認証を実現することが出来る。

【0020】この図1の構成による方式の場合、1つのアプリケーション21がスマートカード22を使用している間このスマートカード22はこのアプリケーション21に専有されるので、他のアプリケーション21は排他が解除されスマートカード22が解放されるまで待ち状態になる。よってこの方式では、複数のアプリケーションの並列処理性能が悪く、また待ち状態にあるアプリケーションは長い期間処理を停止してハングアップした状態に見える等、非常に使い勝手が悪くなる。

【0021】これを回避するものとしては、アプリケーション21がスマートカード22へのアクセス処理が完了すると専有していたスマートカード22を逐一解放する方式がある。この方式では、アプリケーション21が複数回スマートカード22に対するアクセス処理を含む場合、各アクセス処理毎に排他制御機構11に対してスマートカード22への排他獲得／解放を行い、こまめに排他制御を区切る。

【0022】図2に、この方式による各アプリケーションのスマートカードへの排他獲得／解放の例を示す。同図は、図1と同様アプリ1、アプリ2及びアプリ3の3

つのアプリケーション21がカードaに対してアクセス要求を発行した場合の各アプリケーションのスマートカードへのアクセス処理例を示すもので、同図中排他制御機構11への矢印↑は、各アプリケーション21から排他制御機構11への排他獲得要求、排他制御機構11からの矢印↓は排他制御機構11から各アプリケーション21への排他獲得の通知を示す。また斜線部分は各アプリケーション21によるPIN認証処理、網掛け部分はスマートカード22へアクセス処理を示す。

【0023】排他を獲得したアプリケーション21が、全処理が完了するまで排他を解除してスマートカード22を解放しなかった場合、アプリ2は排他制御機構11にカードaへの排他獲得要求を行った図2中の31の位置から、既にカードaへの排他を獲得しているアプリ1が処理が完了する33の位置まで、更にアプリ3は32の位置からこのアプリ2の処理が完了するまで待ち状態となる。しかし、同図の様にアプリケーション21が各アクセス処理毎にこまめに排他制御を区切ることにより、排他が解除された期間に別のアプリケーション21がカードaにアクセスすることが出来るので、排他獲得の待ち状態となり処理が停止してしまう期間が短くなり、処理の並列性が向上する。

【0024】この様に、排他制御を頻繁に切替えると、各アプリケーションの待ち状態の期間は短くなり処理の並列性は向上する。しかし図2の斜線部に示すように各アプリケーションは切替えの度に認証状態の設定／解除処理を行う必要があり、その為のオーバーヘッドが大きくなってしまふ。また認証の再許可を得る際PINを送信するので、各アプリケーション21がPINを保持し続けることになり、セキュリティ上の問題も生じる。これを回避するため、認証処理の度にユーザがパスワードを入力する構成とすると更に認証処理のオーバーヘッドが大きくなる。

【0025】図3にこの点を考慮した構成を示す。図3の構成では、複数のアプリケーション21とスマートカード22の間に、排他制御機構11に加えアクセス制御機構12を設け、このアクセス制御機構12によって各アプリケーション21のスマートカード22による認証を一元管理しながら、排他制御機構11がスマートカード22にアクセスするアプリケーション21の排他処理を行っている。

【0026】各アプリケーション21はスマートカード22に対してアクセスを要求する際、まず排他制御機構11に対して排他獲得要求を行い、排他が獲得できると次にアクセス制御機構12にスマートカード22への認証を依頼する。そして認証が得られるとスマートカード22内のデータにアクセスする。

【0027】アクセス制御機構12は認証状態管理テーブルを持ち、この認証状態管理テーブルを用いてアプリケーション21がスマートカード22への認証の開始宣

言を行ってから認証の解除を通知するまでの間について各アプリケーションとスマートカード22との認証状態の管理を行う。

【0028】図4は、認証状態管理テーブルの構成例を示す図である。認証状態管理テーブルは、各アプリケーション21が現在どのスマートカード22から認証を得ているのかを排他制御機構11が管理するために用いるテーブルで、アプリ識別情報と認証済みカード情報を対応づけて記憶している。アプリ識別情報は、各アプリケーション21を識別するための一意な識別子を記憶するもので、この識別子は、一般のアプリケーションが操作できないものが用いられ、例えばプロセス生成時に各プロセスに付加され、カーネルが管理しているプロセスIDを用いる。あるいは、スマートカードへアクセスへのアクセス要求を行ったアプリケーション21に対してアクセス制御機構12が識別子を順次生成付加してゆく構成としてもよい。

【0029】図4はカードa、bの2つのスマートカード22に対する各アプリケーション21の認証状態を管理する場合を例示しており、各アプリケーションに対し認証済みカード情報としてそのアプリケーション21が認証されているカードが記録されている。尚認証済みカード情報が空欄の部分は、そのアプリケーションに対し認証済みとなっているスマートカードが存在しないことを示す。同図では、アプリ1はカードa、b両方が認証済み、アプリ2、アプリnはいずれも未認証、アプリ3はカードaのみ認証済みとなっている。

【0030】各アプリケーション21は、スマートカード22に対する認証及びスマートカード22へのアクセスをアクセス制御機構12を介して行う。アプリケーション21からスマートカード22へのアクセス要求があると、認証状態管理テーブルを参照してそのアプリケーション21がアクセス要求したスマートカード22に認証済みであるかどうかを調べ、未認証ならばアプリケーション21からの要求を拒絶し、またアプリケーション21にPINの入力を要求してスマートカード22との認証処理を行う。また、そのアプリケーション21が認証済みならばアプリケーション21は既にそのスマートカード21の認証許可を得ているのでスマートカード21へのアクセスを許可し、実行する。

【0031】図5はアプリケーション21がスマートカード22へのアクセスを行う際の、アプリケーション21、排他制御機構11及びアクセス制御機構12の処理の流れを示した図である。同図はアプリ1がカードaに対してアクセスを行う場合を例としており、また以下の説明中の1)～23)は図5中の番号と対応している。

1) アプリ1はカードaへの排他開始を行うため、排他制御機構11に対し、排他獲得要求を行う。

2) アプリ1からの要求に対し、排他制御機構11は、カードaに対し排他獲得済のアプリケーションが有るか

調べ、既に他のアプリケーションが獲得していたならば排他待ちのキューに登録する。また排他獲得済でなければ、アプリ 1 に排他獲得を通知する。

3) アプリ 1 は、アクセス制御機構 12 にカード a へのアクセス開始宣言を行う。

4) アクセス開始宣言に対しアクセス制御機構 12 は、認証状態管理テーブルにアプリ 1 を登録する。そして、アプリ 1 に P I N の入力要求を行う。尚アプリ 1 がカード b にもアクセス開始宣言を行っている場合は、アプリ 1 は既に認証状態管理テーブルに登録してあるのでカード a に対するアクセス開始宣言で再度認証状態管理テーブルに登録する必要はない。

5) アプリ 1 はユーザにパスワードの入力を促し、ユーザの入力から P I N を指定してカード a への認証を要求する。

6) 排他制御機構 11 は、カード a に対し P I N を通知し、カード a に認証チェックを行わせる。

7) アクセス制御機構 12 は、カード a による認証チェックの結果、認証が得られれば、認証状態管理テーブルにアプリ 1 がカード a に認証済みであることを登録する。

8) アプリ 1 はアクセス制御機構 12 に対し、カード a へのデータの読み出し／書込みを要求する。

9) アプリ 1 からの読み出し／書込み要求に対し、認証状態管理テーブルを検索し、アプリ 1 が認証済カード a に認証済みならばカード a に対してアクセスを行う。未認証ならば、アプリ 1 にエラーを通知する。

10) 1 つのアクセス処理が完了しカード a の専有を解除する場合に、アプリ 1 は排他制御機構 11 に排他の解除を通知する。

11) 排他制御機構 11 は、登録されているアプリ 1 のカード a に対する排他獲得を削除し、他にカード a への排他待ちのキューに登録されているアプリケーション 21 があればそのアプリケーション 21 の排他獲得を登録する。

12) 排他の解除後、アプリ 1 はカード a へのアクセス処理以外の処理を行う。この間、カード a の排他を解放しているので他のアプリケーション 21 がカード a を使用することが出来る。

13) アプリ 1 は、再度カード a へのアクセスの必要が生じると、排他制御機構 11 に排他獲得要求を行う。

14) アプリ 1 からの要求に対し、排他制御機構 11 は 2) と同様、カード a に対し排他獲得済のアプリケーションが有るか再度調べ、既に他のアプリケーションが排他獲得済でなければ、アプリ 1 に排他獲得を通知する。

15) アプリ 1 はアクセス制御機構 12 に対し、カード a へのデータの読み出し／書込みを要求する。

16) アクセス制御機構 12 は、再度 9) と同様な処理を行う。この時 7) で、認証状態管理テーブルにアプリ 1 がカード a に認証済みであることが登録されているの

で、そのままカード a へアクセスを行う。以降アプリ 1 内のカード a へのアクセス処理の回数分 10) ~ 16) の処理が繰り返される。

17) 全アクセス処理が完了するとアプリ 1 は、アクセス制御機構 12 にカード a への認証を解除を通知する。

18) アクセス制御機構 12 は、認証状態管理テーブルのアプリ 1 からカード a 認証済の情報を削除する。

19) アクセス制御機構 12 は、認証状態管理テーブル 13 に他にカード a に認証されているアプリケーション 21 が存在しなくなるまで認証状態を保持し、認証されているアプリケーション 21 が存在しなくなるとカード a に認証解除を要求する。これにより同一のスマートカードとの認証処理の回数を削減することが出来る。

20) アプリ 1 は、アクセス制御機構 12 にスマートカード 22 へのアクセス終了を通知する。

21) 20) での通知を受けるとアクセス制御機構 12 は認証状態管理テーブルから、アプリ 1 を削除する。この時アプリ 1 が他のスマートカード 22 に対してはまだアクセスを終了していない場合は認証状態管理テーブルからアプリ 1 を削除しない。

22) アプリ 1 は排他制御機構 11 にカード a の排他の解除を通知する。

23) 排他制御機構 11 は、再度 11) と同様な処理を行い、排他を解除する。

【0032】図 6 は、図 3 の排他制御機構 11 及びアクセス制御機構 12 を備えた構成による各アプリケーションのスマートカードへの処理を示す図である。同図は、比較のため図 2 と同じ前提の元での同じアプリケーション 21 の処理を示してある。図 6 を図 2 と比較すると、各アプリケーション 21 は、認証処理としては、一番最初のカード a へのアクセス処理開始時の P I N による認証処理と、一番最後のアクセス処理終了時にカード a への認証の解除処理を行っているのみで、図 2 では行っていたカード a への各アクセス処理毎の認証処理が省略されている。よって各アプリケーション 21 は認証処理が省略された分処理時間が短くなる。また各アプリケーション 21 が、カード a を専有している期間も認証処理が省かれた分だけ短くなるので、その分待ち状態となる期間が短くてすむ可能性がある。更に各アプリケーション 21 は、スマートカード 22 に対する P I N 認証を最初に 1 度だけ行えばよいので、カードから認証が得られれば P I N を破棄することが出来る。

【0033】図 7 は、本システムによりスマートカード 22 にアクセスを行うアプリケーション 21 の処理を示すフローチャートである。尚これらの処理を行う機構をアプリケーション 21 に直接持たせる構成とすることも出来るが、これらの処理をライブラリとして実現し、このライブラリを各アプリケーション 21 に組込む形態を取るのが一般的な構成である。

【0034】アプリケーション 21 は、スマートカード

22にアクセスを行う際、まず排他制御機構11へ排他獲得の依頼を行い(ステップS1)、排他制御機構11からの応答を待つ。その結果、排他制御機構11から何等かの理由で、排他が獲得出来ない旨の通知が有れば(ステップS2、NO)、処理を終了する。

【0035】排他獲得の依頼に対し、排他制御機構11から排他獲得成功の通知が有れば(ステップS2、YES)、次にステップS3として、アクセス制御機構12にスマートカード22へのアクセスの開始宣言を行う。

【0036】このスマートカード22へのアクセスが未認証のスマートカード22へのアクセスであり、スマートカード22への認証が必要なためアクセス制御機構12からPINの入力を要求された時(ステップS4、YES)、ステップS8としてPINとしてユーザが入力したパスワードをアクセス制御機構12に送って、認証処理を依頼し確認を行う。その結果認証されれば(ステップS9、YES)、処理をステップS5に移してスマートカードへアクセスし、認証されなければ(ステップS9、NO)、処理を終了する。

【0037】ステップS4において、このアクセスが既に認証を得ているスマートカード22へのアクセスである時(ステップS4、NO)、更なる認証処理は必要無いので、ステップS5としてスマートカード22へのアクセスを許可してデータの読み出し/書き込みを行う。

【0038】ステップS5のアクセス処理が終了すると、ステップS6として、アクセス制御機構12に対してスマートカード22へのアクセスの終了宣言を行う。そしてステップS7として、そのスマートカード22への排他の解除を排他制御機構11に通知してスマートカード22へのアクセス処理を終了する。

【0039】図8は、アプリケーション21からの排他獲得要求に対する排他制御機構11の処理を示すフローチャートである。アプリケーション21から、スマートカード22への排他獲得要求があると、排他制御機構11は、ステップS11として、排他獲得を要求されたスマートカード22が、既に他のアプリケーション21によって排他獲得済みであるかどうかを判断する。その結果他のアプリケーション21による排他獲得が行われていなければ(ステップS11、NO)、そのスマートカード22を排他獲得済みとして登録し、要求を行ったアプリケーション22に排他獲得を通知して処理を終了する。

【0040】またステップS11で他のアプリケーション21が排他獲得済みであるならば(ステップS11、YES)、ステップS12としてこの排他獲得要求を排他待ちキューに追加して処理を終了する。

【0041】図9は、アプリケーション21からの排他の解除通知に対する排他制御機構11の処理を示すフローチャートである。アプリケーション21からスマートカード22への排他の解除通知を受けると、排他制御機

構11は、ステップS21としてそのアプリケーション21の排他獲得済みの登録を削除して排他を解除する。

【0042】そして排他待ちキューを調べ、排他が解除されたスマートカード22に対して排他待ちとなっているアプリケーション21が存在すれば(ステップS22、YES)、排他待ちキューの先頭に登録されているアプリケーション21のそのスマートカード22への排他獲得を登録してスマートカード22をディスパッチした後、また排他待ちキューに待ちが存在しなければ(ステップS22、NO)そのまま、処理を終了する。

【0043】図10は、アプリケーション21からのスマートカード22へのアクセス要求に対するアクセス制御機構12の処理を示すフローチャートである。アプリケーション21からのアクセス開始宣言に対し、アクセス制御機構12は、ステップS31として、認証状態管理テーブルにアプリケーション21を登録して、スマートカード22に対してアクセス要求プロセスを登録する。

【0044】図11は、アプリケーション21からのスマートカード22へのアクセス要求に対するアクセス制御機構12の処理を示すフローチャートである。アプリケーション21からのアクセス要求に対し、アクセス制御機構12はステップS41として認証状態管理テーブルを参照して、そのアプリケーション21がアクセス要求先のスマートカード22から既に認証済であるかどうか調べる。その結果、既に認証済みであれば(ステップS41、YES)、更なる認証は必要無いので、ステップS45としてアプリケーション21に対してアクセス許可を通知する。

【0045】ステップS41で、そのアプリケーション21がまだ認証を得ていないのならば(ステップS41、NO)、認証処理を行う必要があるので、ステップS42としてアプリケーション21にパスワードの入力を要求し、スマートカード22に対してPINによる認証チェックを依頼する。その結果、スマートカード22から認証が得られれば、ステップS45としてアプリケーション21に対してアクセス許可を通知し、また認証が得られなければ(ステップS43、NO)、アクセス不許可をアプリケーション21に対して通知して処理を終了する。

【0046】図12は、本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。本実施形態でのアプリケーション41とスマートカード42との間を管理するアクセス管理システム40は、スマートカードリーダー43と各アプリケーション41のライブラリ44との間に構成され、OSの一機能として、あるいはOSに実装される形で実現される。

【0047】アプリケーション41は、スマートカード42に対する認証処理やアクセス処理を、全てこのアクセス管理システム40を介して行い、アクセス管理シス

テム40は、各アプリケーション41とスマートカード42との間のやり取りを把握している。またアクセス管理システム40は、スマートカードリーダ43の状態も把握しており、例えばスマートカードリーダ43からスマートカード42が抜かれると、認証状態管理テーブルを調べ、そのカードが認証済みとしているアプリケーションがあれば未認証に変更する。

【0048】なお、アクセス管理システム40は、内部に排他制御機構11とアクセス制御機構12を別々に持つ構成となっているが、これらを1つの機能構成要素として実現することもできる。また、セキュリティ上、アクセス制御機構や排他制御機構は、複数のアプリケーションが共有できる必要があるので、OSのカーネル内に実現するとセキュリティをより向上することができる。

【0049】図13は、本実施形態における上記スマートカードのアクセス管理をコンピュータプログラムにより実現した場合の情報処理装置のシステム環境図である。スマートカードを実装した情報処理装置は、図13の様にCPU51、ROM、RAMによる主記憶装置52、補助記憶装置53、ディスプレイ、キーボード等の入出力装置(I/O)54、LANやWAN、一般回線等により他の情報処理装置とネットワーク接続を行うモデム等のネットワーク接続装置55、ディスク、磁気テープなどの可搬記録媒体57から記憶内容を読み出す媒体読取り装置56及び1乃至複数のスマートカード59を実装しているスマートカードリーダ58を有し、これらが互いにバス60により接続される構成を備えている。

【0050】また図13の情報処理システムでは、媒体読取り装置56により磁気テープ、フロッピー(登録商標)ディスク、CD-ROM、MO等の記録媒体57に記憶されているプログラム、データを読み出し、これを主記憶装置52またはハードディスク55にダウンロードする。そして本実施形態による各処理は、CPU51がこのプログラムやデータを実行することにより、ソフトウェア的に実現することが可能である。

【0051】また、この情報処理装置では、フロッピーディスク等の記録媒体57を用いてアプリケーションソフトの交換が行われる場合がある。よって、本発明は、スマートカードのアクセス管理システムや共有方法に限らず、コンピュータにより使用されたときに、上述の本発明の実施の形態の機能をコンピュータに行わせるためのコンピュータ読み出し可能な記録媒体57として構成することもできる。

【0052】この場合、「記録媒体」には、例えば図14に示されるように、CD-ROM、フロッピーディスク(あるいはMO、DVD、リムーバブルハードディスク等であってもよい)等の媒体駆動装置77に脱着可能な可搬記録媒体76や、ネットワーク回線73経由で送信される外部の装置(サーバ等)内の記憶手段(データ

ベース等)72、あるいは情報処理装置71の本体74内のメモリ(RAM又はハードディスク等)75等が含まれる。可搬記録媒体76や記憶手段(データベース等)72に記憶されているプログラムは、本体74内のメモリ(RAM又はハードディスク等)75にロードされて、実行される。

【0053】(付記1) 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段とを備えることを特徴とするアクセス管理システム。

【0054】(付記2) 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする付記1に記載のアクセス管理システム。

【0055】(付記3) 前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒絶することを特徴とする付記1又は2に記載のアクセス管理システム。

【0056】(付記4) 前記アクセス制御手段は、アプリケーションとスマートカードとの認証関係を該アプリケーションのプロセスIDを用いて管理することを特徴とする付記1乃至3のいずれか1に記載のアクセス管理システム。

【0057】(付記5) 前記アクセス制御手段は、前記スマートカードがスマートカードリーダより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする付記1乃至4のいずれか1に記載のアクセス管理システム。

【0058】(付記6) 前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする付記1乃至5のいずれか1に記載のアクセス管理システム。

【0059】(付記7) 前記排他制御手段は、アプリ

ケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする付記6に記載のアクセス管理システム。

【0060】（付記8） 前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする付記1乃至7のいずれか1に記載のアクセス管理システム。

【0061】（付記9） 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【0062】（付記10） 1つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであって、複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそのライブラリ。

【0063】（付記11） 1つスマートカードへの複数のアクセス処理を含むアプリケーションのライブラリであって、複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーションのライブラリ。

【0064】（付記12） 複数のアプリケーションが並列動作する情報処理装置によって使用された時、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマ

ートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【0065】

【発明の効果】本発明によれば、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション単位の認証を可能とする。

【0066】また、各アプリケーションとスマートカードとの間の認証関係が一元管理されているので、アプリケーションがスマートカードにアクセス要求を行うとそのスマートカードはそのアプリケーションを認証済みかどうか判断され、未認証の場合のみ認証処理が行われるので、認証処理回数を削減することが出来、認証処理によるオーバーヘッドを小さくすることが出来る。またPINによる認証処理は、最初に一度だけ行われるのでアプリケーションは、PINを保持し続ける必要がなく、セキュリティレベルの向上が図れる。

【0067】更にスマートカードは、認証状態を保持したまま複数の認証済みアプリケーションとの間でアクセスが可能となる。またアプリケーションは、排他獲得の為の待ち状態期間を短く出来る。よって処理の並列性を向上出来また各アプリケーションの処理時間の短縮を図れる。

【図面の簡単な説明】

【図1】排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図である。

【図2】排他制御機構を備えた構成時の各アプリケーションのスマートカードへのアクセス処理を示す図である。

【図3】排他制御機構及びアクセス制御機構を設けた場合の構成図である。

【図4】認証状態管理テーブルの構成例を示す図である。

【図5】アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、排他制御機構及びアクセス制御機構の処理の流れを示した図である。

【図6】排他制御機構及びアクセス制御機構を備えた構成時の各アプリケーションのスマートカードへのアクセス処理を示す図である。

【図7】スマートカードにアクセスを行うアプリケーションの処理を示すフローチャートである。

【図8】アプリケーションからの排他獲得要求に対する排他制御機構の処理を示すフローチャートである。

【図9】アプリケーションからの排他の解除通知に対する排他制御機構の処理を示すフローチャートである。

【図10】アプリケーションからのスマートカードへの

アクセス開始宣言に対するアクセス制御機構の処理を示すフローチャートである。

【図 11】アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャートである。

【図 12】本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。

【図 13】情報処理装置のシステム環境図である。

【図 14】記憶媒体の例を示す図である。

【図 15】スマートカード内部の論理的構成を示す図である。

【符号の説明】

11 排他制御機構

12 アクセス制御機構

21、41 アプリケーション

22、42、59 スマートカード

40 アクセス管理システム

43、58 スマートカードリーダー

51 CPU

52 主記憶装置

55 補助記憶装置

54 入出力装置

55 ネットワーク接続装置

56 媒体読取り装置

57 可搬記憶媒体

60 バス

71 情報処理装置

72 記憶手段

73 ネットワーク回線

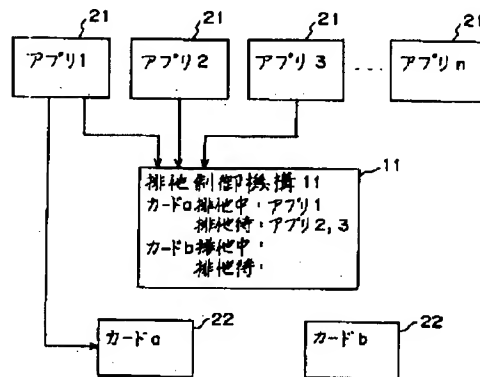
74 情報処理装置本体（コンピュータ）

75 メモリ

76 可搬記録媒体

【図 1】

排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図



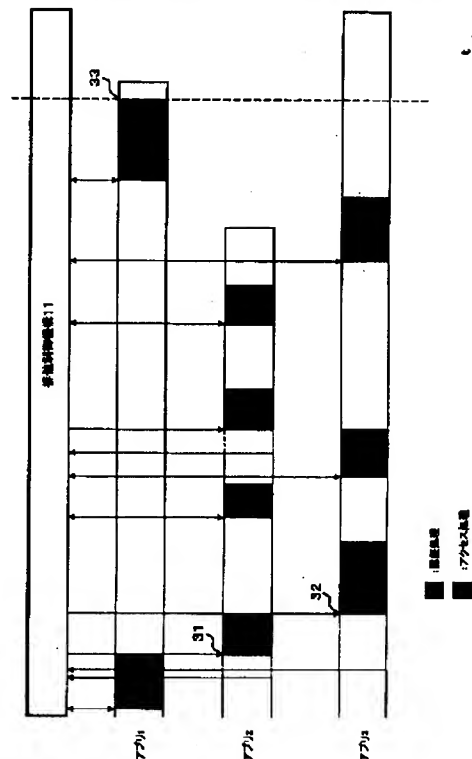
【図 4】

認証状態管理テーブルの構成例を示す図

アプリ識別情報	認証済みカード情報	
アプリ1	カードa	カードb
アプリ2		
アプリ3	カードa	
.....
アプリn		

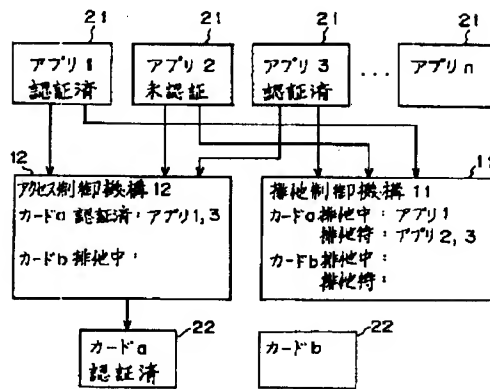
【図 2】

排他制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図



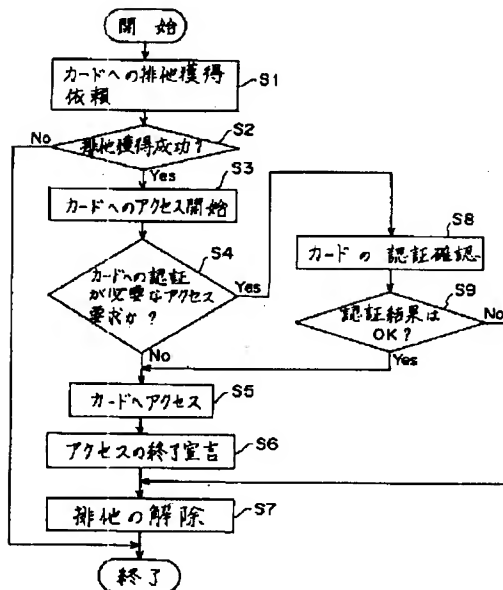
【図3】

排他制御機構及びアクセス制御機構を
設けた場合の構成図



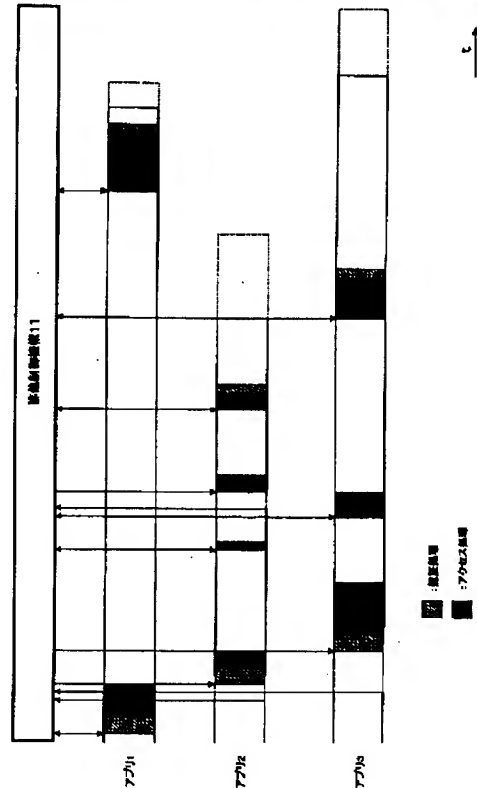
【図7】

スマートカードにアクセスを行うアプリケーションの
処理を示すフローチャート



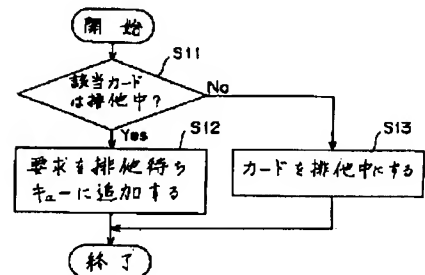
【図6】

排他制御機構及びアクセス制御機構を備えた構成時の
各アプリケーションへのスマートカードへのアクセス処理を示す図



【図8】

アプリケーションからの排他獲得要求に対する
排他制御機構の処理を示すフローチャート



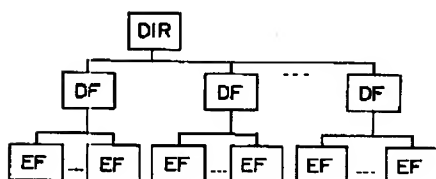
【図5】

アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、
排他制御機構及びアクセス制御機構の処理の流れを示した図



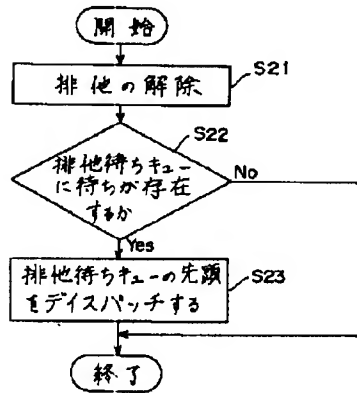
【図15】

スマートカード内部の論理的構成を
示す図



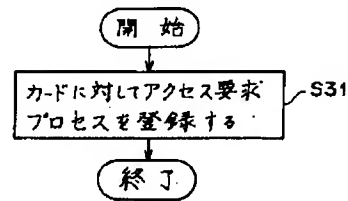
【図9】

アプリケーションからの排他解除通知に対する排他制御機構の処理を示すフローチャート



【図10】

アプリケーションからのスマートカードへのアクセス開始宣言に対するアクセス制御機構の処理を示すフローチャート

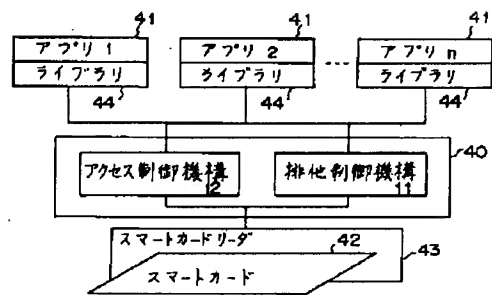
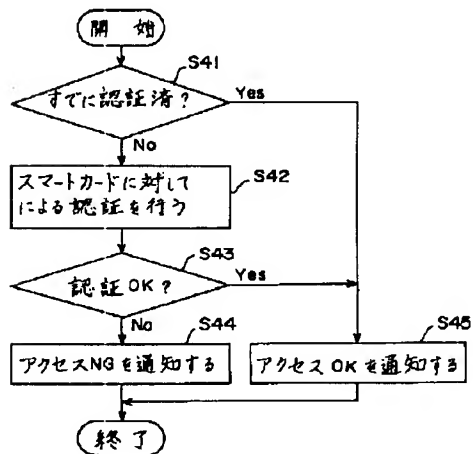


【図12】

本実施形態に於けるスマートカードを使用するシステムの構成を示す図

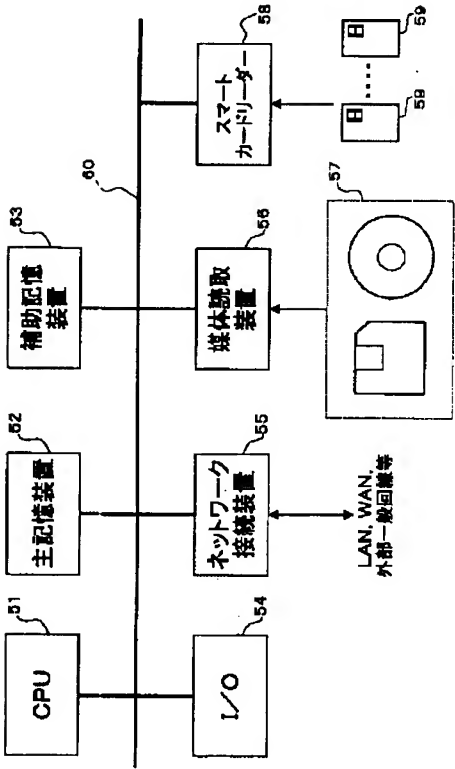
【図11】

アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャート



【図13】

情報処理のシステム環境図



【図14】

記憶媒体の例を示す図

